

Digital Forensics Myanmar

Digital Forensics Myanmar

Digital Forensics Myanmar is the first blog for digital forensics in Myanmar. This blog describes basic digital forensics technology and outlines a first responder guide in the Myanmar language.

Aung Zaw Myo (ThirdEye)

www.forensicsmyanmar.com

Covid Positive Day -1

(Memory အနေနဲ့ ဖြစ်အောင် Positive ဖြစ်တဲ့နေ့ကနေ Negative ဖြစ်တဲ့အချိန်ထိ ပေါ့ပေါ့ပါးပါး ရေးတာပါ။)

Digital Forensics အတွက် Commercial Tools တွေက ဈေးကြီးတဲ့အတွက် လေ့လာလိုသူတွေ စိတ်ဝင်စားသူတွေအတွက် အဆင်မပြေပါဘူး။ ဒါကြောင့် Commercial လဲ ဖြစ် Free အနေနဲ့လဲအသုံးပြုလို့ရ လက်တွေ့မှာ အသုံးဝင်နိုင်မဲ့

တစ်ခုနဲ့ မိတ်ဆက်ပေးပါရစေ။ အဲဒါကတော့ Paladin LTS ၊ Paladin Edge 32/64

ဖြစ်ပါတယ်။

Free အနေနဲ့ သုံးဖို့ အကောင်အထည် ပြုလုပ်ပြီး Visa , Master Card

တစ်ခုလိုအပ်ပါတယ်။ (ငွေမဖြတ်ပါဘူး Verify ဖြစ်အောင်လုပ်တဲ့သဘောပါ)

US 25 အနည်းဆုံးပေးရပါတယ် တစ်ကယ်ဆို Commercial အတွက် ဒါပေမဲ့ သိပ်မကွာပါဘူး။ ဒါနဲ့ စစ်ရင် စစ်ဆေးတဲ့ ရလဒ်ကို License ဖြစ်လို့ Sumuri မှ အာမခံတယ်ဆိုတဲ့သဘောပါ။

Paladin LTS ကိုတော့ Triage အနေနဲ့ရော Acquisition အနေနဲ့ပါ အသုံးချနိုင်ပါတယ်။ Paladin LTE မှာ Live Boot တက်ပြီး စစ်ဆေးဖို့ Autopsy ပါဝင်ပါတယ်။

အခြား Open Source Tools တွေလဲပါဝင်ပါတယ်။

Paladin Edge 32/64 ကတော့ Acquisition အတွက် သီးသန့်ဖြစ်ပါတယ်။

Live Boot ဖြစ်တဲ့အတွက် Secure Boot, T2, FileValue ထည့်ထားရင်တော့ သုံးလို့မရပါဘူး။

3 ခုစလုံးကို Multi Boot လုပ်ထားပြီး အသုံးပြုလို့ရပါတယ်။

Paladin LTS တစ်ခုနဲ့တင် ရပါတယ် တစ်ကယ်ဆို သူ့မှာက Acquisition အတွက် နည်းလမ်းပိုစုံလင်ပါတယ်။

3 ခုစလုံးက Ubuntu ကို Modified လုပ်ထားတာဖြစ်ပါတယ်။

ဈေးလဲအရမ်းမကြီး Linux Command နဲ့ အကျွမ်းမဝင်တဲ့ သူတွေအတွက် သီးသန့်ပြုလုပ်ထားတာဖြစ်ပါတယ်။

Window, Mac တွေမှာ Password မသိပဲ စစ်ဆေးဖို့ကြုံလာတဲ့အခါ။ Triage သို့မဟုတ် Acquisition အတွက် ရည်ရွယ်တာဖြစ်ပါတယ်။

Boot CD တွေ Konboot တွေနဲ့ သဘောတရား မတူပါ။

(Operation System မှာ Password ဖျက်တာတွေ။ User Account နောက်တစ်ခု ထပ်ထည့်တာတွေက အချို့နိုင်ငံများမှာ Law နဲ့ မညီတဲ့အတွက် ဖြစ်ပါတယ်။)

#ForensicsMyanmar

Covid Positive Day -2

World No 1 Mobile Forensics Tools ဖြစ်တဲ့ Cellebrite ကနေ မကြာခင် CTF လုပ်ဖို့ရှိပါတယ်။ အဖွဲ့လိုက် သို့မဟုတ် Individual ပြိုင်လို့ရပါတယ်။

Phone 3 လုံးနဲ့ Pc 1 လုံးပါဝင်ပါတယ်။ Phone 3 လုံးကတော့

Physical Analyzer နဲ့ စစ်ပေးပြီး မေးခွန်းတွေဖြေပေးရမှာပါ။ Pc အတွက်ကတော့ Any Tools ဖြစ်ပါတယ်။

Physical Analyzer ကတော့ အခုလက်ရှိ Version 7.47 ဖြစ်ပါတယ်။ Physical Analyzerက UFED4 PC and UFED Touch ကနေ Acquisition လုပ်လို့ရတဲ့ Ufed File ကို Analysis လုပ်တဲ့နေရာမှာ အသုံးပြုတာဖြစ်ပါတယ်။

CTF မှာပေးထားတဲ့ Phone image file တွေက UFED4 PC ကနေ Acquisition လုပ်ထားတာဖြစ်ပါတယ်။

Physically Analyzer ကနေပဲ Analysis လုပ်လို့ရပါတယ်။ Cross Platform ဖြစ်တဲ့ Magnet , Oxygen မှာလဲရပါတယ်။ ☺

Open Source နဲ့လဲသုံးလို့ရတာတွေရှိပါတယ်။

Physical Analyzer ရှိပြီးသား ပြိုင်ပွဲဝင်တွေအနေနဲ့ Image File ကို ကြိုပြီး Analysis လုပ်နိုင်တဲ့အတွက် အချိန်ပိုရပါတယ်။ မရှိရင်လဲ ရက်အကန့်အသတ်နဲ့

Physical Analyzer ကို ပေးသုံးမှာ ဖြစ်ပါတယ်။

(UFED ကို စမ်းသပ် အသုံးပြုရတဲ့ အတွေ့အကြုံရတာနဲ့တင်တန်နေပါပြီ။) (မေးခွန်းတွေ မဖြေရင်တောင်မှ စမ်းသပ်ကြည့်သင့်ပါတယ်)

(Open Source နဲ့ နောက်မှ Phone Image File တွေကို စမ်းသပ်နိုင်ပါတယ်။)

Phone Image File တွေထဲမှာ size ကြီးတာ 2 ခုပါတဲ့အတွက် i7 , Ram 16 to 64 လောက်မှ အဆင်ပြေပါမယ်။ မဟုတ်ရင် Loading လုပ်နေတဲ့ အချိန်က ပိုကြာပါတယ် အဖြေရှာရတဲ့ အချိန်ထက်။

(Phone Image File ကို Physical Analyzer မှာ Loading လုပ်ပြီးရင် Project File ကို Save ထားပါ။ တစ်ခုခုကြောင့် စက်ဟန့်သွားရင် အစကနေ ပြန်လုပ်နေရတာကြောင့် အချိန်ပိုကုန်နိုင်ပါတယ်။)

PC အတွက်ကတော့ E01 image File ကို ပေးထားမှာ ဖြစ်တာကြောင့် Autopsy လိုမျိုး FTK Imager လိုမျိုးသုံးရင် အဆင်ပြေပါတယ်။

Phone 3 လုံးနဲ့ PC 1 လုံးက ပေးထားတဲ့ အမှုအပေါ်မူတည်ပြီး တစ်ခုနဲ့တစ်ခု ဆက်စပ်နေပါလိမ့်မယ်။ တစ်ချို့အဖြေတွေကဆက်စပ်ပြီး ရယူရတာတွေပါပါတယ်။

(Physical Analyzer , Image File တွေက အနည်းဆုံး GB 100 Down ရဖို့ ရှိပါတယ်။) Edited

(CTF ကလဲ ရက်ပိုင်းလောက်လိုသေးတဲ့အချိန် Physical Analyzer အသုံးပြုပုံနဲ့ သူနဲ့ပတ်သတ်တာတွေကို Website တွေ YouTube တွေမှာ ကြိုပြီး လေ့လာထားနိုင်ပါတယ်။)

အသေးစိတ် Link

<https://www.cellebrite.com/en/the-all-new-cellebrite-capture-the-flag-ctf/>

#UFED #Write_Up_2020

<https://ciofecaforensics.com/2020/10/30/cellebrite-ctf/>

<https://www.cellebrite.com/en/cellebrite-capture-the-flag-follow-up-our-experts-review-the-questions-and-answers/>

Good Luck

#ForensicsMyanmar

2021 - Cellebrite Mobile Forensics CTF Write Up

Write Up ရေးတဲ့ ၂ ယောက်က UFED Physically Analyzer , UFED Inspector မသုံးပဲ Autopsy , ArtEx ကို အဓိက အသုံးပြုထားကို တွေ့ရပါတယ်။

Link -1

<https://medium.com/@williamskosasi/cellebrite-ctf-2021-writeup-b73d821a708>

Link-2

<https://www.stark4n6.com/2021/10/cellebrite-ctf-2021-heisenbergs-android.html?m=1> Positive Day -3

GrayShift's GrayKey ကို UFED, Magnet တို့မှာ ပါဝင်ပါတယ်။ phone image file ကို load လုပ်တဲ့အချိန်မှာ Graykey ကို ရှိခဲ့ရင် ထည့်ပေးရတာဖြစ်ပါတယ်။ သီးခြား Product တစ်ခုဖြစ်ပါတယ်။

GrayShift Company က လူအယောက် ၅၀ ခန့်သာရှိပေမဲ့ Product နဲ့ပတ်သတ်ရင် Secret အရမ်းဖြစ်ပါတယ်။

GrayShift's GrayKey က US နဲ့ ပါတနာကျတဲ့ နိုင်ငံတွေမှ Law Enforcement Agency Only ကိုပဲ ရောင်းချတာဖြစ်ပြီး ဝယ်တဲ့သူက NDA ထိုးရပါတယ်။ Iphone ကို Lock ဖြေပေးဖို့ Apple ကိုတောင်းဆိုတဲ့ အခါတုန်းက မဖြေပေးတဲ့အတွက် ကြားကနေ lock ဖြေပေးတာက GrayShift က ဖြေပေးခဲ့တာဖြစ်ပါတယ်။

Iphone and android phone တွေရဲ့ Passwords ကို

Brute force Attack နဲ့ ရယူနိုင်ပါတယ်။ (Apple ကတော့ IOS 12 နောက်ပိုင်း Password ကို Graykey နဲ့မရယူနိုင်ဘူးလို့ဆိုပါတယ်။)

ဒါပေမဲ့ ခုထိ GrayShift ကလဲ ထုတ်ဖော်ပြောကြားခြင်းမရှိပါ။ Phone Image ကို UFED ထဲကို Loading လုပ်တဲ့အချိန်မှာ ထည့်ရတဲ့ Graykey ကတော့ Crack လို့ရတဲ့ Password သို့မဟုတ် Hash ပဲ ဖြစ်ပါတယ်။ ဒါမှ Phone OS ကနေ Encryption လုပ်ထားတာတွေကို ဖြေလို့ရမှာဖြစ်ပါတယ်။

နောက်ပိုင်း GrayShift's GrayKey မှာ Social Engineering အတွက်ပါ ပါဝင်လာတယ်လို့တော့ သိရပေမဲ့ အပြည့်အစုံတော့ မသိရပါ။

Social Engineering နည်းတစ်ခုကတော့ Lock ဖြစ်နေတဲ့ ဖုန်းကို GrayKey Device နဲ့ချိတ်ဆက်ပြီး Agent (bot) ထည့်ပြီးရင် Suspect ကို မိသားစု သို့မဟုတ် ရှေ့နေနဲ့ဆက်သွယ်စေရန် ဖုန်းပြန်ပေးတာဖြစ်ပါတယ်။ User ရိုက်သွင်းတဲ့ Passcode ကို Agent မှတ်သားထားပါတယ်။

(Lock Phone ထဲကို Agent ထည့်လို့ရအောင် Graykey မှာ ဘယ်လိုလုပ်ထားလဲတော့ မသိပါ။)

Link

<https://www.grayshift.com/>

Positive Day -4

Pladin LTS, EDGE 32/64 မှာ Support လုပ်တဲ့ Image Type များ

DD (Raw)

EWf v1 (Expert Witness Format)

EWf v2

SMART (ASR data Image Format)

DMG (Apple Disk Image)

VMDK (Use For Virtual View)

(Forensics Mode နဲ့ Live လုပ်တဲ့အခါ Computer ထဲကို ချိတ်ဆက်တဲ့ Storage Media တွေက Read Only Mode အနေနဲ့ဖြစ်သွားမှာ ဖြစ်ပါတယ်။)

Support လုပ်တဲ့ Function တွေကတော့

- Forensics Imaging

- Cloning The Drive

- Imaging Across The Network

(NAS,Raid ရှိခဲ့လျှင်)

- Converting Forensics Image Type to Another Forensics Image Type

- Imaging Unallocated Space and unpartitioned Space

(Triage နည်းလမ်းမှာ အသုံးဝင်ပြီး ဖျက်ထားတဲ့ File တွေကို ပြန်ရနိုင်ပါတယ်။)

- Logical Imaging

(Only Image Folder and File)(Can't Recovery From This Image)

- Image and File Hashing

- Mounting , Unmounting (Read only, RW Only)

- Restore Forensics Image Back To Physical Disk

- Bitlocker Decrypt (Need Password)

- Triage (Keywords,File Name, Content Name, MIME ဖြင့် မှုရင်း Device ကို ပုံစံမပျက်စေပဲ ရှာဖွေခြင်း။)

(Pladin မှာ Investigation Log File ပါဝင်တဲ့အတွက် Live Boot စတင်တဲ့အချိန်ကတည်းမှ စပြီး လုပ်သမျှကို မှတ်တမ်းရှိနေမှာ ဖြစ်ပါတယ်။)

Sorry I can't post details Screenshots this moment 😞

Positive Day - 5

(Toilet ဝင်ရင် Confidence Level ဆိုးဟိုက်နေဆဲ 🤔)

Android ရဲ့ Internal Memory ထဲကနေ ဖျက်လိုက်တဲ့

Dialer (Call Log), Contact, SMS, App Data တို့ကို သာမန်သုံးနေကြ Recovery App တွေနဲ့ Recovery ယူလို့လုံးဝမရပါဘူး။ Internal Memory ရဲ့ Raw Partition ကို ဝင်ဖို့ Data Extraction လုပ်ဖို့အတွက် Root Access လိုအပ်ပါတယ်။

Root Access ရဖို့ဆိုတာကလဲ အခု Android Version အမြင့်ပိုင်းတွေမှာ မလွယ်ကူတော့ပါ။ အရင်က Myanmar Fonts ပေါ် ဖို့ Browser မှာ မြန်မာလိုပေါ် ဖို့ Root လုပ်ခဲ့တဲ့ အချိန်တွေကို မေ့ထားလိုက်ပါ။

Root လုပ်လို့ရနိုင်ခဲ့ရင်လဲ Root လုပ်တဲ့ Process မှာ Android ရဲ့ /data မှာ File အချို့နေရာသွားယူပါတယ်။ အဲဒီအတွက် အရေးကြီးတဲ့ Data တွေက Flash Memory ရဲ့ Unlocated Space ကနေ ပျောက်သွားတတ်ပါတယ်။ ဥပမာ Delete Sms or Delete Call Log

SD Card က File တွေဆိုရင်တော့ရတယ် ဖုန်းကျရင်လဲ ရရမှာပေါ့ မေးစရာရှိပါတယ်။ SD Card File System က FAT32 ပါ။ Forensics Tools တင်မကပါဘူး တောကနေ မြို့အထိသုံးတဲ့ Recovery App တောင် FAT32 ကို Recovery ရပါတယ်။ 😊

Android Version အနိမ့်တွေမှာ YAFFS2 အခုနောက်ပိုင်းတွေမှာ EXT3, EXT4, RFS File System တွေသုံးပါတယ်။ သုံးနေကျ Recovery App တော်တော်များများက အဲဒီ File System တွေကို Support မလုပ်နိုင်ပါဘူး။

Phone ရဲ့ System App တွေဖြစ်တဲ့ Dialer (Call Log), SMS, Contact နဲ့ App Data တွေဖြစ်တဲ့ Browser History စတာတွေက Phone ထဲမှာ SQLite Format နဲ့ သိမ်းဆည်းတာဖြစ်ပါတယ်။ Supportd Phone Forensics App တွေကပဲ Recovery လုပ်ယူလို့ရနိုင်ပါတယ်။ ဒါတောင် လွဲချော်သွားမှာတွေ ရှိနိုင်လို့ Manual Carving လုပ်ချင်လုပ်ရပါတယ်။ Commercial Forensics App တွေက SQLite ရဲ့ Unlocated Block, Free Block တွေထဲကနေ Recovery လုပ်တာဖြစ်ပါတယ်။ Data လုံးဝမရှိတဲ့ လုံးဝရှင်းနေတဲ့ Defaults ဖြစ်သွားတဲ့ SQLite ထဲမှာတော့ ဘာဆိုဘာမှ မရနိုင်ပါ။ God ပဲသိနိုင်မဲ့ အရာဖြစ်သွားပြီး။ ☹️

တော်တော်များများ Recovery App တွေက ဖုန်းကို Root မှ ရမယ်ဆိုတဲ့ အချက်ကို သိပ်မပြောကြပါဘူး။

#ForensicsMyanmar

Positive Day -6

(အနံနဲ့ ပတ်သတ်ရင် ကွန်ဖီးဒန့် Level ဆိုးဟိုက်နေဆဲ ☹️)

I phone မှာလဲ Dialer (call), SMS , Calendar, Contact, Event, Mail, Note တို့ကို SQLite Database နဲ့ပဲ သိမ်းဆည်းပါတယ်။

.sqllitedb .db extension အနေနဲ့ အများဆုံးတွေ့ရမှာ ဖြစ်ပါတယ်။အဲလို file extension မရှိတာတွေ။ Write-Ahead Log (WAL) တို့လဲ ရှိပါတယ်။

ဥပမာ

Contact ဆိုရင် AddressBook.sqlitedb

Call history ဆိုရင် callHistory.storedata

Sms ဆိုရင် sms.db

Note ဆိုရင် notes.sqlite

Safari အတွက် Bookmarks.db, History.db

အရင် ယခု သုံးခဲ့ သုံးနေတဲ့ Sim Card Data တွေကို

CellularUsage.db ထဲမှာတွေ့နိုင်ပါတယ်။

SQLite File တွေကို ဖတ်ဖို့ Recovery လုပ်ဖို့အတွက်

Open Source Tools တွေရှိပါတယ်။ Unlocated Space, Free Space ကနေပါ ရှာဖတ်ဖို့ Recovery လုပ်ဖို့အတွက်က Commercial ကပိုအဆင်ပြေတယ်လို့ ပြောကြပါတယ်။

ဥပမာ ကျွန်တော်ကနေ ဝတ်မှုန်ရွှေရည်ကို လမ်းခွဲကြောင်း SMS စပို့လိုက်တယ်။ မကြာခင် Mဆိုင်လုဆီက Sms ဝင်လာတာနဲ့ တစ်ခြားသူဆီက ဝင်တာနဲ့

အဲ့ဒီ Sms က ဖုန်းထဲမှာ အောက်ရောက်နေရင်းနဲ့ မပေါ်တော့ဘူး။ sms.db မှာက limit Storage ရှိပါတယ်။ အဲ SMS က sms.db ထဲမှာတော့ ရှိနေဆဲပါ။

နောက်တစ်ခါ

ပို့ပြီးတာနဲ့ အမြင်ကပ်စွာနဲ့ပဲဖျက်လိုက်တယ်။ အဲဒီ SMS က sms.db ထဲမှာရှိနေသေးပါတယ်။ ဒါပေမဲ့ Operator ကဝင်လာတဲ့ SMS တွေ အခြားသူဆီကနေဝင်လာတဲ့ SMS တွေကြောင့် Sms.db မှာ Storage လိုပြန်ပါတယ်။

အခြေအနေအရ နောက်တစ်ခါ အမှတ်တရ အနေနဲ့ ပြန်ရှာမယ်ဆိုရင် ရှိချင်မှ ရှိပါတော့မယ်။

(ဒါကြောင့် ဖုန်းစသိမ်းရင် airplane Mode On ရတာပါ။)(Phone Storage က Flash Memory သုံးထားပါတယ်။)(System App ဖြစ်တဲ့ Call, Contact, Sms SQLite File တွေက Default ဖြစ်သွားရင်တော့ God ပဲ သိနိုင်မဲ့ အခြေအနေပါ။)

Sqlite File တွေတင်မက Property Lists (plist) file တွေကနေလဲ အချက်အလက်တွေရရှိနိုင်ပါတယ်။ Plist က ခြုံပြောရရင် Phone System နဲ့ ပတ်သတ်တဲ့အချက်အလက်တွေ ရရှိနိုင်ပါတယ်။

ဥပမာ (Itune back up Restore date) (Wireless History.)

#ForensicsMyanmar

Positive Day -7

အနံ့နဲ့ပတ်သတ်ရင် ကွန်ဖီဒန့် လယ်ဗယ် So High 🙄

လှုပ်ရှားတာနဲ့ အရင်လိုမဟုတ် မောပန်းလွယ်လာတယ်။

Android Version 6 ကနေစပြီးရင် Full Disk Encryption (FDE) ကိုစတင်လာပါတယ်။ User ရဲ့ data တွေကို Secret Key နဲ့ Encrypt လုပ်လိုက်ပါတယ်။ Secret Key ကို User ပေးထားတဲ့ Pin, Password နဲ့ ထပ်ပြီး Encrypt ထပ်လုပ်ထားပါသေးတယ်။ Flash Memory ပေါ်မှာ သွားမသိမ်းခင်ကတည်းက user ရဲ့ data တွေကို Encryption လုပ်ထားလိုက်ပါတယ်။ ဒါက Chipoff အတွက် အခက်အခဲ ဖြစ်လာစေပါတယ်။

Android Version 7 ကနေစပြီးရင် Android Verify Boot စတင်ပါဝင်လာပါတယ်။ Normal Mode အနေနဲ့ Phone Operation System တက်လာဖို့ Partation နဲ့ Segment တွေမှာ အဆင့်တိုင်း Integrity ရှိ မရှိ စစ်ဆေးပါတယ်။ တစ်ခုခုကို ပြင်ထားမယ်ဆိုရင် Integrity မမှန်ဘူးဆိုရင် Normal Mode အနေနဲ့ Boot တက်လာမှာ မဟုတ်ပါဘူး။ ကွန်ပျူတာမှာ UEFI ပုံစံနဲ့ ဆင်တူပါတယ်။

Android Version 7 နဲ့ နောက်ပိုင်းမှာ File Base Encryption (FBE) ပါဝင်လာပါတယ်။ File အားလုံးအတွက် Encryption Key တစ်ခုထဲမဟုတ်ပဲ File တစ်ခုချင်းစီကို Encryption Key တစ်ခုစီ ဖြစ်လာပါတယ်။

Full Disk Encryption (FDE) မှာတုန်းကလို File အားလုံးကို Decrypt လုပ်ဖို့စောင့်စရာမလိုတော့ပါ။ ဒါကြောင့် Notification အချို့ကို User က Phone ကို Unlock မလုပ်ထားရင်တောင်မှ Screen မှာ မြင်နေရတာပါ။

Android 7 နဲ့ နောက်ပိုင်းမှာ File Base Encryption ပါဝင်လာတဲ့အတွက် (FBE) ပါတဲ့ ဖုန်းတွေမှာ Root Access ရဖို့မလွယ်ကူတာပါ။နောက်ပိုင်း Boot Loader Unlock လုပ်ရတာတွေ ။ Boot Loader Unlock လုပ်ရရင် Phone က Reset ကျတဲ့ အတွက် Root လုပ်ဖို့ မလွယ်ကူတော့ပါ။ Recovery ပိုင်းအတွက် Challenge တွေ ဖြစ်လာစေပါတယ်။

Custom Recovery Methods အသုံးပြုရင်တော့ ရနိုင်ပါတယ်။ ဘာလို့လဲဆိုရင် Android ရဲ့ Recovery Partation မှာ Root Access ရှိလို့ဖြစ်ပါတယ်။

နောက်ပိုင်း Commercial Mobile Forensics Tools တွေမှာ CWM, TWRP တို့လုပ်ဖို့အတွက် အဆင့်တွေ။ CWM, TWRP ကနေရလာတဲ့ File တွေကို Analysis လုပ်ဖို့အတွက် ပါဝင်လာပါတယ်။ ဒီအဆင့်တွေကို ကျော်ပြီး(အသုံးမပြုပဲ)

အသုံးပြုလို့ရပေမဲ့ ကျွမ်းကျင်အောင် လေ့လာထားသင့်ပါတယ်။

Forensics မှာ Data ရရှိက အရေးကြီးဆုံး အချက်ဖြစ်ပါတယ်။

#ForensicsMyanmar

Positive Day -8

အနံ့ပျင်းတဲ့အရာတွေဆို ပီစီလေး အနံ့ရ 🍷

Commercial Tools ကနေ ဖော်ပြတာတင်မဟုတ်ပဲ SQLite File တွေကို Analysis လုပ်မယ်ဆိုရင် IOS Devices တွေမှာသုံးထားတဲ့ Time-stamp တွေကို သိထားဖို့လိုအပ်ပါမယ်။

Unix Time Stamp

January 1 1970 မှစတင်ပါတယ်။ millisecond, Nanosecond တွေနဲ့ ဖော်ပြတတ်ပါတယ်။ Time ပြောင်းဖို့ online/offline Tools တွေရှိပါတယ်။

Unix Time Stamp ကို IOS Devices တွေမှာ အများဆုံးသုံးပါတယ်။

Mac Absolute Time

IOS-5 ကနေစတင်အသုံးပြုပါတယ်။

January 1 2001 မှ စတင်ပါတယ်။

WebKit/Chrome Time

January 1 1601 မှာ စတင်ပါတယ်။

Commercial Tools တွေမှာတော့ အလိုအလျောက် Time ကို ပြောင်းလဲပေးတာတွေရှိပါတယ်။

#ForensicsMyanmar

Positive Day - 9

(ပုံမှန်အလုပ်တွေပင် မောပန်းလွယ်သည်။)

iphone ရဲ့ file system တစ်နည်းအားဖြင့် Logical Partation ကို 2 ပိုင်းခွဲခြားထားပါတယ်။

System (Root/Firmware) နဲ့ နောက်တစ်ခုက User Data တွေရှိနဲ့ User Data Partation အပိုင်း။

System Partation မှာ IOS နဲ့ Preloaded Application တွေပါဝင်ပါတယ်။ System Partation က Read Only အနေနဲ့ပဲ ရှိပါတယ်။ ဒါပေမဲ့ IOS Upgrade လုပ်နေတဲ့ အချိန်နဲ့ Device Jailbroken ဖြစ်နေရင်တော့ Read Only မဟုတ်တော့ပါဘူး။ Android Phone က အရင်ကဆို Root ပြီးရင်လဲ Un root လုပ်လို့ရပေမဲ့ Idevices ကတော့ တစ်ခါ Jailbreak လုပ်ပြီးရင် Forever Jailbreak ဖြစ်နေမှာ ဖြစ်ပါတယ်။

System Partation က Firmware Upgrade လုပ်နေတဲ့အချိန်ပဲ Update ဖြစ်နေမှာ ဖြစ်ပြီး Update လုပ်တဲ့အချိန်မှာ Itune က Partation တစ်ခုလုံးကို Userdata တွေကို မထိခိုက်ပဲ Format လုပ်ပါတယ်။

System Partation size က Phone ရဲ့ Nand Flash ပေါ်မူတည်ပြီး 0.8 GB - 4 GB အထိရှိပါတယ်။

အပေါ်မှာပါတဲ့အတိုင်း Firmware Upgrade လုပ်တဲ့အချိန်အထိပဲ System Partation က update လုပ်တာဖြစ်ပြီး ကျန်တဲ့အချိန်မှာတော့ စက်ရုံက ထုတ်လိုက်တဲ့ အခြေအနေအတိုင်းပဲ ရှိနေမှာ ဖြစ်ပါတယ်။ Evidence အနည်းသာ System Partation ကရရှိနိုင်ပါတယ်။

Jailbreak Device တွေ မှာတော့ System Info တင်သာမက User Data အချို့ပါ System Partation ကနေရရှိနိုင်ပါတယ်။ (Jailbreak Info ပါရရှိနိုင်ပါတယ်။)

Iphone 5 ကနေစပြီး Apple Encryption စနစ်ကြောင့်

Physical Acquisition ရယူမဖြစ်နိုင်တော့ပါဘူး။ Commercial Forensics Tools တွေကလဲ Logical Acquisition သာအဓိက Support ပေးပါတယ်။ Filesystem Acquisition နဲ့ DFU Mode ကနေ Acquisition လုပ်မယ်ဆိုရင် Idevices ကို Jailbreak လုပ်ရပါတယ်။

CTF တွေ Exercise တွေမှာ ပေးထားတဲ့ Phone Image တွေက Jailbreak လုပ်ထားတဲ့ Device တွေက နေယူထားတာဖြစ်ပါတယ်။ Acquisition နည်းလမ်းနဲ့ လုပ်တာမတူတဲ့အတွက် Extraction လုပ်ပြီးအခါ ရလာတဲ့ Results ရော Analysis လုပ်တဲ့နေရာမှာ ရရှိတဲ့ Results တွေမှာ Jailbreak မလုပ်တဲ့ Device နဲ့ ကွာခြားနိုင်ပါတယ်။

User Data Partation မှာတော့ User ကနေ Create လုပ်တဲ့ data တွေနဲ့ Third Party App က data တွေကို သိမ်းဆည်းထားပါတယ်။ ဒါကြောင့် Nand Flash Memory ရဲ့ Size တော်တော်များများကို User Data Partation က အဓိကယူထားပါတယ်။ User Data Partation ကို Mount လုပ်မယ်ဆိုရင် /private/var အနေနဲ့ မြင်တွေ့ရမှာ ဖြစ်ပါတယ်။

Most Of Evidence Information တွေက User Data Partation မှာ အများဆုံးတွေ့နိုင်ပါတယ်။ ဥပမာ Gallery, Note

#ForensicsMyanmar

Positive Day 10

UFED CTF မှာ Itune Backup တွေ PC တွေပါလာတာတွေ့လို့ပါ။

Working With Itunes Backup

Iphone 13 မထွက်ခင် Elcomsoft (Russia Mobile Forensics Product CEO က Iphone 13

ထွက်လာတော့မှာ ဖြစ်တဲ့အတွက် လူတွေက Icloud backup တွေလုပ်ပြီး ဖုန်းတွေချိန်းတော့မှာ ဖြစ်ကြောင်းပြောကြားခဲ့တယ်။

Itune Bckup ကိုလုပ်တဲ့သူရှိသလို မလုပ်တဲ့သူလဲရှိနိုင်ပါတယ်။ လူအပေါ်မူတည်တာပေါ့။ Itune Backup မှာက အရင်က data တွေအပြင် By Passed Certificate နဲ့ Lock Down Certificate တွေပါနိုင်ပါတယ်။ (Password မလိုပဲ login ဝင်လို့ရတဲ့ အနေအထားပါ။)

နောက်ပိုင်း Apple Watch Information ကလဲ Itune Backup ထဲမှာပါလာပါတယ်။

Itune Backup Acquisition

Itune Backup ကိုတော့ အခြား Acquisition Methods တွေအသုံးမပြုနိုင်တဲ့ အခါမျိုးမှာ အသုံးပြုကြတာများပါတယ်။ Itune ကို ကောင်းကောင်းအသုံးပြုတတ်ဖို့ပဲ လိုအပ်ပါတယ်။ Commercial Tools တွေမှာလဲ Itune Backup ကို အလွယ်တကူ Analysis လုပ်နိုင်ပါတယ်။ Open source Tools တွေလဲ ရှိပါတယ်။ Forensics Purpose အတွက် Itune Backup လုပ်တဲ့နေရာမှာ အရေးကြီးတဲ့ အချက်ကတော့ (Encrypt Local Backup) ကို Itune မှာ အမှန်ခြစ်ပေးဖို့ပဲဖြစ်ပါတယ်။

Encrypted Backup လုပ်မှသာ Passwords, WiFi Setting, Web Browsing History တို့ပါဝင်မှာ ဖြစ်ပါတယ်။

Itune Backup On Window & Mac Computer

User ကနေ Data တွေပျက်မှာစိုးလို့ပဲ ဖြစ်ဖြစ် အခြားအကြောင်းအရင်းတစ်ခုခုကြောင့်ပဲ ဖြစ်ဖြစ် သူတို့ ကွန်ပျူတာမှာ Backup ထားတတ်ပါတယ်။ iCloud မှာလဲ backup ထားနိုင်ပါတယ်။

တစ်ကယ်လို့ User Phone က Wipe Or Reset လုပ်ထားရင်တောင် Evidence တွေက Itune Backup Or iCloud မှာ ရှိနေနိုင်ပါတယ်။ Wipe လုပ်လိုက်တဲ့အခါမှာ Apple Encryption ပျက်သွားတဲ့အတွက် Data တွေကို ပြန်ပြီး Recovery မရနိုင်ပါ။

(Can't Recovery Data From Itune Backup)

Window မှာတော့ Itune Backup ရဲ့ Default Location နေရာက

C-Users -Username-AppData-Roaming-
AppleComputer-MobileSync-Backup

MacOS မှာတော့ Itune Backup ရဲ့ Default Location နေရာက

Home-Library-Application-MobileSync-Backup

အသုံးပြုသူတော်တော်များများက Click - Click နဲ့ပဲ Install လုပ် Backup လုပ်ကြတာများလို့ Default Location ကို မှတ်သားရတာဖြစ်ပါတယ်။

Default Location ပြောင်းတာ Backup Name ပြောင်းတာကတော့ အသုံးပြုသူအပေါ်မူတည်ပါတယ်။

Itune နဲ့ Backup လုပ်တဲ့ ပထဆုံးအချိန်အခါမှာ Itune က Backup Directory ကို Create လုပ်ပြီး Idevices ကို Fully Backup လုပ်ပါတယ်။ နောင်အခါ 2nd, 3rd, 4th, etc ... လုပ်တဲ့ အချိန်မှာတော့ Itune က

အရင်ရှိနေပြီးသား Data တွေကို Backup မလုပ်တော့ပဲ အခုအနေအထားမှာ Modified ဖြစ်တဲ့ Data (ယခင် Itune Backup မှာ မရှိတဲ့ Data) တွေကိုပဲ Backup လုပ်ပါတယ်။

Itune Backup ရဲ့ Default Backup Name ကတော့

[Unique Device Identifier (UDID)- (ISO Date)- Time(24H Format)]

Idevices ရဲ့ UDID နဲ့ Backup လုပ်တဲ့ ရက်စွဲ အချိန်တို့ ဖြစ်ပါတယ်။

Itune Backup မှာ ဘာတွေပါသလဲဆိုရင်

SIM card info, Contacts, SMS, Photo, Calendar, Music, Call log, Configuration Files, Keychain, documents, network settings, Web Cache, bookmarks, Cookies, App Data, တို့ပါဝင်ပါတယ်။

(App Data မှာ User Selected App Info ပဲ ပါဝင်မှာပါ)

အကယ်လို့ User က Backup လုပ်တဲ့အချိန်မှာ Itune မှာ Encrypted Backup ကို မရွေးခဲ့ဘူးဆိုရင်တော့ Password တွေမပါပါဘူး။

Standard File In ITune Backup

IOS 10 ကနေစပြီး Itune Backup မှာ ပါဝင်လာတဲ့ Standard File 4 ခုကတော့

Info.Plist

Manifest.Plist

Mainfest.db

Status.Plist

info.plist - Details About Backup Device Information

Manifest.Plist - Contents Of The Backup

Mainfest.db - SQLite Database

Status.Plist - Deatail About Backup Status

ကျွန်တော် နောက်နေ့ တစ်ခုချင်း ရေးသားပါမယ်။

#ForensicsMyanmar

Positive Day - 11

Mobile Forensics Challenge

Hardware Difference

အသုံးပြုတဲ့သူ တစ်ဖြည်းဖြည်းများလာတာနဲ့အမျှ ထုတ်လုပ်တဲ့ Company တွေကနေ User တွေရဲ့ အကြိုက် ငွေတတ်နိုင်မှု အပေါ်ကိုလဲ မူတည်။ ပြီးရင် ထုတ်လုပ်တဲ့ Company အချင်းချင်းပြိုင်ဆိုင်မှုတွေကြောင့် Mobile Phone ထုတ်လုပ်မှုကို Short Product Development Cycle အနေနဲ့သာထုတ်လုပ်ပါတယ်။

Mobile Operation System

လူအများ သုံးနေတဲ့ Window, Mac တွေလိုမဟုတ်ပဲ

Mobile Operation System တွေက Product အလိုက် Operation System အမျိုးမျိုးကွဲပြားပါတယ်။

ဥပမာ

Android အပေါ်မှာ အခြေခံပေမဲ့ MI ဆို တစ်မျိုး Samsung ဆိုတစ်မျိုး စသည်ဖြင့်ကွဲပြားပါတယ်။

Mobil Security Platform Features

အစဦးပိုင်း Android Version တွေလိုမဟုတ်ပဲ အသုံးပြုသူတွေရဲ့ Security and Privacy တွေကို
အလေးပိုထားလာတာကြောင့် Forensics အပိုင်းမှာ အခက်ခဲတွေရှိလာပါတယ်။ Encryption တွေက
Hardware Layer တင်မက Software Layer အထိပါ ပါဝင်လာတဲ့အတွက် အရင်ကလို မလွယ်ကူတော့ပါ။

Anti Forensics Techniques

Factory Reset, Secure Wiping , Data- Obfuscation, Data Forgery, Data Hiding, Cloud Storage
တွေကြောင့်ပို အခက်ခဲရှိလာပါတယ်။

Passcode Recovery

Phone Service နဲ့ မတူတာက Forensics လုပ်တဲ့နေရာမှာ Passcode လဲကျော်ရုံတင်မက အဓိက
အရေးကြီးတဲ့ အတွင်း Data တွေကို မပျက်စီးစေဖို့ပါ။

Different Product နဲ့ Different OS တွေကြောင့် ရတာရှိသလို မရတာလဲ ရှိပါတယ်။

Lack Of Resources

Commercial Mobike Forensics Product တွေရှိပေမဲ့ Open Source နည်းပါးပါတယ်။ အသုံးပြုရတဲ့ ပစ္စည်းတွေလဲအများကြီးလိုအပ်ပါတယ်။ Commercial တွေဈေးကြီးရခြင်း အကြောင်းအရင်းက လတိုင်းထွက်ရှိနေတဲ့ Mobile Phone တွေကို Research လုပ်ပေး Product မှာထည့်ပေးရတဲ့ Research စာရိတ်ပါ ပေါင်းယူတာကြောင့်ပါ။

ကျန်တာတွေကတော့

Accidental Reset and Clear Cache, Dynamic nature Of Evidence, Device Alteration, Communication Shielding, တို့ပဲဖြစ်ပါတယ်။

#ForensicsMyanmar

Sorry For Details ,ဖုန်းကနေပဲ စာရိုက်ရေးနေရလို့ပါ။

Positive Day - 12

Android Backup

Commercial Tools တွေမှာတော့ Click & Click သွားဖို့လွယ်ပြီး User ကလဲ အသုံးပြုရတာလွယ်ကူပါတယ်။

ဒါပေမဲ့ Behind The Scenes Commercial Tools နောက်ကွယ်က လုပ်သွားတာတွေ ဘာလို့ ဒီလိုရလာတယ်ဆိုတာတွေ ဘာကြောင့် ဒီလိုရလာတယ်ဆိုတာကို တော်တော်များများသတိမပြုမိကြပါဘူး။

Adb Backup (Using Adb Command)

Google က Android Version 4 ကနေစပြီး Adb Backup ကို အသုံးပြုခွင့်ပေးလာပါတယ်။

Adb Command ကို Window, Linux ,Mac တွေမှာ အသုံးပြုလို့ရပါတယ်။

ပြည်ပ LEA တွေသုံးတဲ့ Mobile Forensics Commercial Product တွေမှာ Data Extraction လုပ်ဖို့ Click နှိပ်တာရဲ့ နောက်ကွယ်မှာ အဓိက Run တာက Adb Command တွေပါ။

မယုံရင် Extraction နှစ်ခု လုပ်ပြီး ရလာတဲ့ Data ကို ယှဉ်ကြည့်ပါ။

နောက်ပိုင်းမှာတော့ Adb Command ကနေ Backup ယူတာမှာ အားနည်းချက်တွေရှိလာပါတယ်။ အချို့သော Applications တွေကနေ Data တွေကို Adb Command နဲ့ရယူဖို့ ပိတ်လာပါတယ်။ ဥပမာ Facebook App လိုဟာမျိုးဆိုရင် တော်တော်ကိုရှေးကျနေတဲ့ Facebook App မှာသာ adb Command ကနေ App Data တွေကို ဆွဲယူလို့ရနိုင်ပါတယ်။

ဒါ့ကြောင့် Mobile Forensics မှာ App Down Grade လုပ်တယ်ဆိုတာပေါ်လာပါတယ်။ Downgrade အကြောင်းကို 2020 လောက်မှာ Vlog မှာရေးသားပြီးဖြစ်ပါတယ်။

Content Provider

နောက်ပိုင်း Android တွေမှာ App တစ်ခုက Data ကို ကျန်တဲ့ App ကနေ ရယူလို့ မရပါဘူး။ ဒါပေမဲ့ App တစ်ခုက Data ကို အခြား App မှာသုံးလို့ရအောင် Content Provider (Data Request Permission) တွေရှိပါတယ်။ App တစ်ခု Run တဲ့အချိန်မှာ User ကနေ ဒီ App ကို ဘာ Permission တွေပေးသုံးမယ်ဆိုတာ Access ပေးရပါတယ်။ ဥပမာ Access Contact, Call log , SMS

Commercial Product တွေက ဒီလိုမျိုး Content Provider တွေကိုပါစစ်ဆေးနိုင်ပါတယ်။ နောက်တစ်ခုက ဖုန်းထဲက SQLite Database တွေကို ဖုန်းအမျိုးအစားအလိုက် Recovery လုပ်နိုင်ပါတယ်။ ဒါ့ကြောင့် ဈေးကြီးတာပါ။

Android မှာ Data Acquisition လုပ်ဖို့ Adb Command တွေလဲ စိတ်ရှုပ်တယ် အမှားအယွင်း ရှိမှာစိုးလို့
မသုံးချင်ဘူး။ Acquisition လုပ်ရာမှာသုံးဖို့

Commercial Product လဲမရှိဘူးဆိုရင် အလွယ်ဆုံးက Local Backup ဖြစ်ပါတယ်။ Phone မှာ Local Backup
ကထွက်လာတဲ့ .bak File ထားဖို့

Storage မလောက်ရင် OTG Or SD Card ပဲလိုပါတယ်။ ဒါမှမဟုတ် Computer နဲ့ချိတ်ချင်ချိတ်လို့ရပါတယ်။

(.bak File Cant Recovery Deleted Data)

*(Some Advanced User Protect Password For Local Backup .This Password is not same Device
Login Password)* (But may be same)

.bak File ကို Analysis လုပ်ဖို့ Open Source Or Commercial Product တစ်ခုခုတော့လိုအပ်ပါတယ်။

#ForensicsMyanmar

Positive Day -13

(အနံ့ ကွန်ဖီဒန် လယ်ဗယ် ဆိုးဟိုက် ☹)

2021 ကလဲ ကုန်ခါနီးလာပြီဆိုတော့ 2022 နှစ် မတိုင်ခင် 2021 မှာ မှတ်တိုင်တစ်ခုအနေနဲ့

ရေးလက်စရှိနေတဲ့ Digital Forensics With Autopsy စာအုပ်ကို အပြီးသတ်ပြီး PDF အနေနဲ့ Just For
Knowledge အနေနဲ့ရော Education Purpose အနေနဲ့ရော Free တင်ပေးသွားပါမယ်။

(မြန်မာမှာသာ တန်ဖိုးမရှိပေမဲ့ အခြားနေရာတွေမှာ Course တွေ Training တွေက ဈေး အရမ်းကြီး
ပါတယ်။)

စာအုပ်မှာ

Acquisition အတွက် Commercial Product တွေကထုတ်တဲ့ Acquisition Tools တွေနဲ့ Forensics Image အမျိုးမျိုးရယူပုံ။

Autopsy 8 Hours Training မှာ သင်တဲ့သင်ခန်းစာတွေနဲ့ အခြားပတ်သတ်ပြီးသိသင့်တာတွေ အကုန် အပြီးသတ်ရေးပေးသွားပါမယ်။

အနည်းဆုံး ရရှိမှာတွေကတော့

-Autopsy အပြင် အခြား Commercial Product တွေကို အလွယ်တကူ အသုံးပြုနိုင်သွားပါမယ်။

- နှိုင်းယှဉ်တဲ့ အကြောင်းအရာတွေမှာ Commercial Product တွေအကြောင်းပါ အလျှင်းသင့်သလိုပါဝင်ပါမယ်။

- အခုတစ်လော ရေးထားတာတွေ တစ်စုတစ်စည်းတည်း ဖြစ်အောင် Vlog မှာ Update လုပ်ဖို့လဲရှိပါတယ်။

#ForensicsMyanmar

Positive Day-14

Itune Backup Forensics မှ အဆက်

-----*****-----

info.plist

Info.plist မှာ Backed Up Device နဲ့ ပတ်သတ်တဲ့ အကြောင်းတွေပါဝင်ပါတယ်။

Applications - Device မှာ Install လုပ်ထားတဲ့ App စာရင်း

Build Number - IOS Build Version Number

Device name and Display Name - Device name နဲ့ Owner Name

GUID - Global Unique Identifier

ICCID - Integrated Circuit Card Identifier , SIM Card ရဲ့ Serial Number ,

IMEI - International Mobile Equipment Identity

Last Backup Date - နောက်ဆုံး Successful Backup လုပ်ခဲ့တဲ့ ရက်စွဲ

MEID - Mobile Equipment Identifier

Phone Number - Backup လုပ်တဲ့အချိန်မှာ အသုံးပြုတဲ့ ဖုန်းနံပါတ်

Product Name - Eg, Iphone 11,12

Product type , Product Version (Firmware Versions) , Phone Serial Number, UDID, Itune Version

Itune Setting - Delete App Information

-----*****-----

manifest.plist

Backup Contacts နဲ့ ပတ်သတ်တာတွေပါဝင်ပါတယ်။

Backup Keybag - Backup လုပ်တဲ့ ဖုန်းမှာပဲ Itune Backup လုပ်နိုင်ဖို့ Phone Hardware Keys

Version - Backup Version

Date - Backup Create လုပ်တဲ့အချိန် နှင့် Last Update ပြုလုပ်တဲ့ အချိန်

Mainfestkey - manifest.db ကို Encrypt လုပ်ထားသည့် Key

WasPasscodeSet - Last Sync ပြုလုပ်တဲ့အချိန် Passcode ထားခြင်းရှိ မရှိ ဖော်ပြ

Lockdown - Device details နှင့် Last Backup လုပ်တဲ့ Computer Name

Applications - Third Party Application Lists

Is encrypted - Encrypted Backup လုပ်ထား မထား ဖော်ပြ။

-----*****-----

Status.plist

Backup Status ကိုဖော်ပြပါသည်။

IsFullBackup - Fully Backup လုပ်ထားမထား ဖော်ပြ။

Date - Backup Modified နောက်ဆုံးပြုလုပ်တဲ့ အချိန်။

BackupState - New Backup လား ဒါမှ မဟုတ် အရင် Backup ကို Modified လုပ်ထားတာလား ဆိုတာကိုဖော်ပြ။

(ပထမဆုံးအကြိမ်သာ Fully Backup လုပ်ပြီး နောက်တစ်ကြိမ်ထပ်လုပ်ရင် အရင် Backup မှာ မရှိတဲ့ Data ကိုပဲ Backup လုပ်ပါတယ်။)

SnapshotState - Backup Procee Successful ဖြစ်တာကို ဖော်ပြ။

-----*****-----

manifest.db

Backup မှာ ပါဝင်တဲ့ Files, Folders List တွေကို SQLite Database အနေနဲ့ ဖော်ပြ။

FieldID - SHA1 Hash နဲ့ Files Folders Path တွေကို ဖော်ပြ။

Domain - files Folders တွေကို iOS မှာ Domain အမျိုးမျိုးနဲ့ ခွဲခြားထားပါတယ်။ eg, Home Domain, Camerarolldomain

File - file ထဲမှာ Plist File တွေပါဝင်ပြီး အဲဒီ Plist file တွေက Last Modified Time , File Birth Time တွေကို Unix Time Stamp နဲ့ ဖော်ပြပါတယ်။

#ForensicsMyanmar

Positive Day - 15

Lock Down File

(For Passcode Protect Idevices)

Idevices နဲ့ Computer ချိတ်ဆက်တဲ့ အခါ Computer မှာ Lock Down File ကို Plist File အနေနဲ့ Itune က Automatic Create လုပ်လိုက်ပါတယ်။

Lockdown File ကို Paring Record လို့လဲ ခေါ်ပါတယ်။ Idevices နဲ့ ချိတ်ဆက်တဲ့ Computer ရဲ့ကြားက Trusted Record လဲဖြစ်ပါတယ်။

(အချို့ Mobile Forensics Commercial Product အချို့မှာ Lock Idevices အတွက် Lock ကျော်ဖို့ LockDown File Input လုပ်တဲ့နေရာပါပါတယ်။)

(Commercial Product မရှိလဲ Forensics လုပ်မဲ့ PC မှာ Itune Install လုပ်ပြီး ချိတ်ဆက်ဖူးတဲ့ ကွန်ပျူတာကနေ LockDown File ကိုရှာထည့်ပါ။)

LockDown File Location

Window

C:\ProgramData\Apple\Lockdown

MAC

/var/db/lockdown

ဒါပေမဲ့ ကန့်သတ်ချက်အချို့တော့ ရှိပါတယ်။

1 - Seized လုပ်လိုက်တဲ့ Locked Apple Device နဲ့ အတူ ချိတ်ဆက်ဖူးတယ်လို့ယူဆရတဲ့ Computer ပါ Seized လုပ်တဲ့အထဲမှာ ပါဝင်ရမယ်။ မချိတ်ဆက်ဖူးရင် Lockdown File မရှိပါ။

2 - Seized လုပ်ပြီးတဲ့နောက်ပိုင်း Phone ကို Don't Restart, Don't Power Off

(ဘာလို့လဲဆိုရင် Phone ကို Restart Or Power off

လုပ်ပြီး အနည်းဆုံး တစ်ကြိမ် Passcode ကို Unlock ပေးမှ ရမှာဖြစ်တာကြောင့်ပါ။)

3- Jailbreak Device မဖြစ်ရပါဘူး။

IOS Security Feature With Lock Down File

IOS 8 and Lower - Working

IOS 9 To 11 - Working

IOS 11 To 11.3 - Require Password For Connect

IOS 11.3 and Above - Password ကို တစ်ပတ်ကို တစ်ကြိမ်တော့ ရိုက်ရမည်။ Time Expiration

IOS 11.4 and Above - Computer နဲ့ ချိတ်ဆက်ပြီး ပြန်ဖြုတ်လိုက်တဲ့ နောက်ပိုင်း တစ်နာရီကျော်တာနဲ့ Passcode ရိုက်ဖို့ User ကို Force ပေးပါတယ်။ Restricted Mode

#ForensicsMyanmar

Positive Day - 16

မနေ့ကရေးခဲ့တဲ့ Sharing App Data to another app , App Install ပြုလုပ်တဲ့အချိန်မှာ ပေးတဲ့ Permission, ဖြစ်တဲ့ Contact Provider ကြောင့် Android ဖုန်းကနေ Forensics အတွက် အရေးကြီးတဲ့ Valuable Data တွေကို ဆွဲယူဖို့ App တစ်ခုရှိပါတယ်။ Develop မဖြစ်တာတော့ကြာပါပြီ။ နောက်ပိုင်း Android Version တွေနဲ့ အဆင်ပြေ မပြေတော့မသိပါ။ ။ ပြန်ပြင်ရေးမယ်ဆိုရင်တော့ ရပါတယ်။

သူ့အလုပ်လုပ်ပုံက Commercial Mobile Forensics Tools အလုပ်လုပ်ပုံနဲ့ ဆင်တူပါတယ်။ ☹️

Github မှာပေးထားတာက Law Enforcement အသုံးပြုဖို့ ပေးထားတဲ့ Version တော့မဟုတ်ပါဘူး။ Law Enforcement Version အတွက် သီးခြား Free ပေးဖို့တောင်းရင်ရတယ်လို့ ပြောပါတယ်။ LE Version က Data ပိုရပါတယ်။ ပြန်ပြင်ရေးမဲ့သူရှိရင် ရှာပြီးတင်ပေးပါမယ်။

Adb Pull Command နဲ့ ဆွဲယူပြီး CVS Format ပြောင်းပြီး Save ပေးတာပါ။

Info.xml မှာတော့ ဖုန်းနံပါတ်သတ်တဲ့ IMEI, IMSI စတဲ့ Device Info တွေပါဝင်ပါတယ်။

Github ကနေယူသုံးကြ ပြင်ရေးကြတာကတော့ No.1 Forensics Product အစွဲရေး Made UFED တောင် ပါပါတယ်။ Research Team ကနေ အသုံးတည့်မဲ့ဟာရှာတယ်။ထပ်ပြီး Research လုပ်တယ်။ ပြန်ပြင်ရေးကြတယ်။

FBI or CIA က လားမမှတ်မိတော့လို့ အဲဒီက လူတစ်ယောက်က ufed မှာ Github ကနေ ယူထားတာ ဘာတွေလဲ ဘယ်လို ပြင်သုံးတယ်ဆိုတာ ရေးဘူးပါတယ်။

AFLogical OSE Link

<https://github.com/nowsecure/android-forensics/downloads>

Sorry SD Card မရှိလို့ Extraction Results ကို ပုံမပြနိုင်တာပါ။

(နောက်ပိုင်း Android Version အတွက်ပြင်ဆင်ရန်သာလိုပါသည်။)

#ForensicsMyanmar

Positive Day - 17

အမှန်တစ်ကယ်က Window 11 မှာ Trusted Platform Module (TPM) ပါမှ တင်လို့ရမယ်လို့ ပါလာတဲ့အတွက်ပါ။ (တစ်ကယ်တော့ TPM မပါလဲ Skipped လုပ်လို့ရပါတယ်။)

အရင်အချိန်တွေကို ပြန်သွားကြည့်ရင်

Pull and Plug Methods

ကျွန်တော်တို့ Desktop Or Laptop မှာ Secure Boot, Bootloader, Login Password Password ခံထားရင် အသုံးပြုတဲ့နည်းပါ။ အချို့နိုင်ငံတွေမှာ

Digital Forensics လုပ်ရင် ဥပဒေ နည်းဥပဒေရှိတဲ့အတွက် Konboot, Boot Disk လိုမျိုးတွေသုံးပြီး User Password ဖျက်တာ User Account နောက်တစ်ခု ထည့်တာတွေ လုပ်လို့မရနိုင်ပါဘူး။ အဲဒီအတွက် Alternative နည်းလမ်းဖြစ်တဲ့ Pull and Plug Methods ကိုအသုံးပြုပါတယ်။

(နောက်ပိုင်း အချို့နိုင်ငံများမှာ Sized လုပ်မဲ့ Digital Device အတွက် Warrant အပြင် Pin, Patter, Password, Biometric အတွက် Warrant ပါထပ်ပြီးပါလာပါတယ်။)

Pull and Plug Methods ဆိုတာ တစ်ခြားတွေ့မဟုတ်ပါဘူး။ Desktop Or Laptop ထဲက Harddisk, SSD ကိုဆွဲထုတ်ပြီး Forensics SOP အတိုင်းပြုလုပ်တာပါ။

ဖွင့်ဖို့ ဖြုတ်ဖို့မလွယ်တဲ့ အခါမှာတော့ ကျွန်တော် အရင်တစ်ပတ်လောက်က ရေးခဲ့တဲ့ Paladin Edge လိုဟာမျိုး တွေသုံးပါတယ်။

(User Password ကို ဖျက်တာ Account နောက်တစ်ခု ထပ်လုပ်တာမလုပ်ဘူးပေါ့။)

တစ်ကယ်လို့ Bitlocker ခံထားတဲ့အနေအထားနဲ့ ကြုံလာခဲ့ရင် ...

(Password ကို User ကိုမေးမယ်ဆိုတာကို ကျော်ထားပါတယ်။)

1 - Sized လုပ်တဲ့အချိန် Device Power ပွင့်နေရင် Ram Dump ပြုလုပ်ဖို့

နည်းလမ်း

(Don't Forget To take pagefile.sys)

(ကွန်ပျူတာဖွင့်ပြီး Bitlocker Password ကို ရိုက်ပြီး Unlock လုပ်တဲ့အချိန်မှာ Password က Ram ထဲမှာ Device Power မပိတ်မချင်းရှိနေမှာဖြစ်ပါတယ်။)

2 - Sized လုပ်တဲ့အချိန် Device Power Off ဖြစ်နေရင် Non Volatile Information တစ်ခုဖြစ်တဲ့ Pagefile.sys ထဲမှာ Bitlocker Key ရှိနေနိုင်ပါတယ်။

3 - (Device က Sleep or Hybernate အနေအထား ဖြစ်နေရင်လဲ Pagefile.sys ကိုပါ ရယူရပါမယ်။

(Pagefile.sys အကြောင်းအရင်က ရေးပြီးပါပြီ။)

ဒါမှမဟုတ် Bitlocker Recovery Key က Microsoft Account ထဲမှာ Save ထားမလား

<https://onedrive.live.com/recoverykey>

Device က AD , Azure AD သုံးရင် AD ထဲမှာရှိမလား

USB Or Print Or Note ထဲမှာ များ ရှိမလား

ဒါတွေတစ်ခုမှ မရဘူးဆိုရင်

Storage ကို Forensics Image ရိုက်ပြီး Offline Password Attack နဲ့ Decrypt လုပ်ဖို့နည်းလမ်းပဲရှိပါတော့တယ်။ အချိန်တော့ယူရမှာ ဖြစ်ပါတယ်။ Social Engineering သုံးရမှာပေါ့။

(Offline Password Attack လုပ်နေတုန်း Storage Media က အကြောင်းအမျိုးမျိုးကြောင့် ပျက်သွားနိုင်တဲ့အတွက် Forensics Image ပြုလုပ်ပြီးမှ Decrypt လုပ်တာဖြစ်ပါတယ်။

#ForensicsMyanmar

Covid day - 18 (Negative) ♥

(Bitlocker + TPM) (Bitlocker + TPM + Pin) အတွက် Forensics Point Of View

(User ဆီက Password, Pin တောင်းမယ်ဆိုတဲ့ အဆင့်ကို ကျော်ထားပါတယ်။)

Trusted Platform Module (TPM) ဆိုတာက Cryptoprocessor တစ်ခုဖြစ်သလို Built-in Memory လဲပါရှိပါတယ်။ Cryptographic Key တွေကို Computer Mother Board နဲ့ ပေါင်းစပ်ပြီး ထိမ်းသိမ်းဆောင်ရွက်ပေးပါတယ်။

TPM က Motherboard Built in အနေနဲ့ပါရှိသလို Support ပေးတဲ့ Motherboard တွေမှာ Module အနေနဲ့ ထပ်ပြီးတပ်လို့ရပါတယ်။

Bitlocker က AES-128 ကို အသုံးပြုပြီး UEFI အတွက် XTS , Legacy Boot အတွက် CBC ကိုအသုံးပြုပါတယ်။ Data တွေကို Volume Master Key

(VMK) နဲ့ Encryption ပြုလုပ်ပါတယ်။

VMK ကို ဘယ်ကနေရနိုင်မလဲဆိုရင်

1 - Bitlocker Password

2 - Encryption Enable ပြုလုပ်တဲ့ အချိန်မှာ Save ထားတဲ့ File, USB, Print, Note, Microsoft Account,

3 - Trusted Platform Module (TPM)

Bitlocker + TPM

TPM ရဲ့အလုပ်လုပ်ပုံက Block Chain ပုံစံနဲ့ ဆင်တူပါတယ်။ System Boot စတင်တဲ့ အချိန်မှာ Chain Of Truth ကိုစတင်လုပ်ဆောင်ပြီး Platform Configuration Register (PCR) - Small Amount Location ထဲမှာသိမ်းဆည်းပါတယ်။

1 - ကွန်ပျူတာကို ပါဝါ စဖွင့်လိုက်တာနဲ့ Computer ROM ထဲမှာသိမ်းထားတဲ့ Static Root Of Truth For Measures (SRTM) က စပြီး Loading ပြုလုပ်ပါတယ်။

SRTM မှ ပထမဆုံး BIOS ရဲ့ Hash Value ကို Calculate လုပ်ပြီး Chain Of Truth ပြုလုပ်ပါတယ်။

ရလာတဲ့ Hash Value ကို Trusted Platform Module (TPM) ထဲက Configuration Register (PCR) ထဲမှာ သိမ်းဆည်းထားလိုက်ပါတယ်။

2 - BIOS စတင်အလုပ်လုပ်ပြီး Storage Partation, Master Boot Record (MBR), Bootloader, ပြီးရင် တစ်ခြားချိတ်ဆက်ထားတဲ့ Configuration တွေဖြစ်တဲ့ Fingerprint Reader, Card Reader တွေရဲ့ Checksum ကို စစ်ဆေးပါတယ်။ PCR ထဲမှာခုနက သိမ်းထားတဲ့ Hash Value နဲ့ ထပ်ပြီးတော့ New Hash Value ရယူပါတယ်။ တစ်ခုခုပြင်ထားမယ်ဆိုရင် Chain တစ်ခုလုံးကို ဖျက်လိုက်ပါတယ်။

3 - Master Boot Record ထဲမှာရှိတဲ့ Bootloader စတင်အလုပ်လုပ်။ လိုအပ်တဲ့ Record ထည့်ပြီးရင် ထပ်ပြီး Hash Value တွက်ထုတ်ပါတယ်။

4 - နောက်ဆုံးဖြစ်တဲ့ OS Kernel အလုပ်လုပ်ပါပြီး။ Kernel ကနေ လိုအပ်တဲ့ Record ကို Chain Of Truth ထဲ ထပ်ထည့်ပါတယ်။

1. (S-CRTM) - 2. (BIOS/UEFI Code) - 3. (Boot Lader)- 4.(OS Kernel)

(Block Chain ပုံစံအတိုင်းသွားပါတယ်။)

TPM ထဲက Configuration Register (PCR) ထဲမှာ Chain Of Truth တွေကို အကုန် ပါဝင်ပါတယ်။ PCR ကိုပြင်ဆင်လို့မရပါဘူး။

(ROM Vulnerability ဖြစ်တဲ့အတွက် အချို့သော IOS Devices တွေမှာ Checkm8 Exploit ဖြစ်ပြီး Password မသိရင်တောင် Data အချို့ကိုဆွဲ ယူနိုင်ပါတယ်။)

Bitlocker + TPM

(Bitlocker key ကို TPM ထဲမှာ သိမ်းထားလိုက်တဲ့အခါ)

User က Bitlocker Enable လုပ်လိုက်တဲ့အခါ Window ကနေ Volume Master Key (VMK), Recovery Key တို့ကို ထုတ်ပေးလိုက်ပါတယ်။

VMK key က TPM ထဲမှာ သိမ်းထားလိုက်ပြီး Recovery Key နဲ့ ထပ်ပြီး Encrypt လုပ်လိုက်ပါတယ်။

Encrypted လုပ်ထားတဲ့ VMK key ကို Disk Header ထဲမှာ သိမ်းထားလိုက်ပါတယ်။

Reboot , Shutdown ကနေပြန်တက်လာတဲ့အခါမှာ

- PCR Register တွေထဲမှာ သိမ်းထားသမျှက မရှိတော့ပါဘူး။

- အပေါ်က အဆင့် ၄ ဆင့်ကို ထပ်ပြီးလုပ်ဆောင်ပါတယ်။

- OS Kernel အဆင့်ကနေ Encrypt လုပ်ထားတဲ့

Storage Partation ကို Unlock လုပ်ဖို့အတွက် TPM ထဲမှာသိမ်းထားတဲ့ Encrypted VMK ကို Request လှမ်းလုပ်ပါတယ်။ TPM ကနေ PCR Register တွေကိုစစ်ဆေးပြီး Chain Of Truth မှန် မှန်စစ်ဆေးပါတယ်။ Corrupt ဖြစ်သွားရင် VMK Key ကို ထုတ်မပေးပါဘူး။

(Bitlocker key ကို TPM ထဲမှာ သိမ်းထားတဲ့အတွက်

Storage ကို Pull လုပ် အခြား Forensics Work Station မှာ တပ်ပြီး Decrypt လုပ်လို့မရတော့ပါဘူး။

လက်ရှိ ကွန်ပျူတာမှာသာ Storage က အလုပ်လုပ်ပါမယ်။ TPM + Storage ကိုဖြုတ်ပြီး အခြား ကွန်ပျူတာမှာလဲ သွားတပ်လို့မရပါဘူး။)

TPM By Pass နည်းလမ်း

1 - Sized လုပ်မဲ့ ကွန်ပျူတာက ပါဝါ ပွင့်နေရင် Sleep Mode ဖြစ်နေရင် Shut Down မလုပ်ပဲ Ram Dump လုပ်တဲ့နည်းလမ်း။

(Sleep Mode ဖြစ်နေရင် TPM ထဲက PCR Register က NVRAM ထဲမှာ ရှိနေပါတယ်။ Wake ဖြစ်တဲ့ အချိန် အဆင်သင့်ဖြစ်အောင်လို့ပါ။)

2 - Memory Image ယူနိုင်တဲ့ Linux ကို Bootable လုပ်ပြီး Memory ယူမဲ့နည်းလမ်း။

Boot password ခံထားခဲ့ရင်

Bitlocker + TPM + Pin ပြုလုပ်ထားရင်။

Seized လုပ်တဲ့အချိန် ကွန်ပျူတာပိတ်ရက် အနေအထား

(Boot Password ကို အကြိမ်ကြိမ်မှားထည့်ရင် TPM က Login လုပ်ဖို့ အချိန်ကို Time Restricted လုပ်လိုက်ပါတယ်။)

(Battery ဖြုတ်ပြီး Time Restricted ကိုကျော်နိုင်ပါတယ်။)

Cold Boot

စောနက OS Kernel ကနေ Encrypted လုပ်ထားတဲ့ Storage ကို TPM ကို Request လှမ်းလုပ်တဲ့အချိန်မှာ Chain Of Truth ကလဲ မှန်နေတဲ့အတွက် VMK Key က Ram ထဲမှာ ရောက်နေပါပြီ။

ကွန်ပျူတာကို Login ရောက်တဲ့အထိ ဖွင့်။ ပြီးရင် ပြန်ပိတ်လိုက်ပါ။ Login နေရာမှာ Encrypted Volume က Mount နေပါပြီ။

ပိတ်ပြီးတဲ့အချိန်မှာ RAM ကို Liquid Nitrogen နဲ့ RAM ကို ရေခဲမှတ်ရောက်တဲ့အထိ မှုတ်လိုက်ပါတယ်။

(Computer Power Off သွားပေမဲ့ RAM ထဲမှာ သိမ်းဆည်းထားတာက အချိန်အတိုင်းအတာ တစ်ခုထိရှိနေပါသေးတယ်)

ရေခဲမှတ်ရောက်အောင် မှုတ်ပြီးရင် အခြား Computer မှာ RAM ကိုချက်ခြင်းတပ်ပြီး Memory Image ယူနိုင်တဲ့ Linux ကို Bootable တပ်ပြီး Image ယူပါတယ်။

(Computer Shutdown ဖြစ်တာနဲ့ Ram ပေါ်က Data မရစေရန် အတွက် Ram ပေါ်ကို Memory Override လုပ်တဲ့နည်းတွေလဲပေါ်နေပါပြီ။

Firewireနဲ့ Thunderbolt နည်းလမ်းကတော့ Window 7, 8.1 မှာ BIOS update မလုပ်ရသေးတာတွေပဲရပါတော့တယ်။

(Sleep Mode and Cold Boot ကတော့ Analysis လုပ်တဲ့အနေနဲ့ 2 ခါလောက်စမ်းသပ်ကြည့်ဖူးပါတယ်။

Sleep Mode မှာအခြေအနေတစ်ခု ရှိပါသေးတယ်။ Wake ဖြစ်လာပြီး ဒါပေမဲ့

Login Password ခံနေတယ်။ အပေါ်ကနည်းလမ်းတစ်ခုခုကို ကိုယ်ကျွမ်းကျင်ရာ ကိုယ့်မှာ ရှိတဲ့ Tools and Capabilities ကိုကြည့်ပြီး လုပ်ရမှာဖြစ်ပါတယ်။

Edited

Memory Overwrite Request Control (MOR) ကြောင့် Ram ထဲမှာ ဘာမှ မကျန်အောင် Overwrite လုပ်လိုက်ပါတယ်။ Attack နည်းလမ်းတွေကို လျှော့ချလိုက်တာပါ။

Link ထဲမှာ ဘယ် Window Version တွေမှာ Support ပေးတယ်ဆိုတာတွေ့နိုင်ပါတယ်။ MOR V2 ဆိုရင်ထွက်တာ လပိုင်းပဲ ရှိပါသေးတယ်။

Full Link

<https://docs.microsoft.com/en-us/windows-hardware/drivers/bringup/memory-overwrite-request-control-lock-version-2>

နောက်ဆုံးတစ်နည်းကတော့ စမ်းသပ်မယ်ဆို ပစ္စည်းရော ငွေကြေးရော လိုအပ်တာကြောင့် မစမ်းသပ်ရသေးပါဘူး။ နည်းလမ်းက TPM Signal ကို Intersection လုပ်တာပါ။ Github မှာ Code နဲ့ နည်းလမ်းရှိပါတယ်။ အောင်မြင်တယ်လို့လဲပြောပါတယ်။

Link

https://github.com/denandz/lpc_sniffer_tpm

#ForensicsMyanmar

Covid Day - 18 (Negative) Post မှာ Edit လုပ်လိုက်တာ မတွေ့လိုက်မှာ စိုးလို့ပါ။

Negative ထွက်တဲ့အထိရေးမယ်လို့ ဆုံးဖြတ်ထားတာမို့ အခုဆို ပြည့်သွားပါပြီ။

ဖုန်းကနေ စာရိုက်ရေးတာဆိုတော့ Details and Screenshot အတွက် ကတော့ Sorry ပါ။

အလုပ်လုပ်ရင်း နားရင်းနဲ့ ရေးလက်စ အဆုံးမသတ်ရသေးတဲ့ Pdf ကို ဖြေးဖြေးချင်း
လက်စသတ်ပါတော့မယ်။

Previous Post မှာ ထပ်ဖြည့်ထားတာပါ။

Memory Overwrite Request Control (MOR) ကြောင့် Ram ထဲမှာ ဘာမှ မကျန်အောင် Overwrite
လုပ်လိုက်ပါတယ်။ခုနက Attack တွေကိုလျှော့ချလိုက်တာပါ။ Link ထဲမှာ ဘယ် Window Version တွေမှာ
Support ပေးတယ်ဆိုတာတွေ့နိုင်ပါတယ်။ MOR V2 ဆိုရင်ထွက်တာ လပိုင်းပဲ ရှိပါသေးတယ်။

Full Link

<https://docs.microsoft.com/en-us/windows-hardware/drivers/bringup/memory-overwrite-request-control-lock-version-2>

နောက်ဆုံးတစ်နည်းကတော့ စမ်းသပ်မယ်ဆို ပစ္စည်းရော ငွေကြေးရောလိုအပ်တာ
ကြောင့် မစမ်းသပ်ရသေးပါဘူး။

နည်းလမ်းက TPM Signal ကို Intersection လုပ်တာပါ။

Github မှာ Code နဲ့ နည်းလမ်းရှိပါတယ်။ အောင်မြင်တယ်လို့လဲပြောပါတယ်။

Link

https://github.com/denandz/lpc_sniffer_tpm

Good Luck Everybody

#ForensicsMyanmar

(Covid Positive Day (1-18) အမှတ်တရ ရေးထားတာပါ။)လိုအပ်ချက်များရှိရင် Sorry ပါ။